

REMARKS

Claims 1-8 remain in the application. Claim 1 has been amended hereby. New claims 8-10 have been added. It is submitted that no new matter has been added and no new issues have been raised by the present Amendment.

In the Office Action, the Examiner has rejected claims 1-8 under 35 U.S.C. § 102(e) as allegedly anticipated by Owens et al. (US 6,338,140).

Independent claim 1 relates to a method for distributing keys to subscribers in digital mobile radio networks. Keys are generated in a security device provided at the mobile radio network end. At least one key is requested from the security device. The at least one key is transmitted via the mobile radio network to a mobile station or a terminal of a subscriber based on the request. The generated keys are stored in the security device prior to transmission. The requesting step is performed by the subscriber. The transmitted key is allocated to the subscriber. The transmitted key is stored in the terminal and/or in a subscriber identity module (SIM) in the mobile station.

Owens et al. does not relate to a method of distributing keys to digital mobile radio network subscribers. Owens et al.

relates to a method and system for validation and/or authentication of the identity of subscribers in a communications network such as a wireless, digital, cellular and/or satellite communications system. A subscriber or user of an insecure communication system enters a random PIN, and a telephone number of whom he wishes to call. The random PIN provides a digital signature to the telephone number. An authentication center authenticates the user by verifying the digital signature and updating a user profile to permit a call only to the telephone number in the sequence dialed by the user.

The Examiner contends that Owens et al. "discloses a method for distributing keys in a security device provided at the mobile radio network end." The Office Action cites col. 3, lines 35-49; col. 7, lines 46-63; col. 13, lines 16-61; col. 16, lines 35-56; and figs. 8-9.

The cited portions of Owens et al. refers to an "individual subscriber authentication key ( $K_i$ )", and a "cryptographic key". These keys appear to be closely related. Owens et al. additionally refers to a "MS 'SND' Key" but this key appears to be a button on a cellular telephone's dial-pad and thus is clearly not analogous to the keys of independent claim 1.

Owens et al. at col. 3, lines 35-40 reads:

The mobile station is uniquely identified by a International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key  $K_i$ , constitutes sensitive identification credentials, analogous to the Electronic Serial Number (ESN) in systems such as AMPS.

When a mobile station MS attempts to access the system, the network issues it a 128-bit random number challenge RAND. The MS computes a 32-bit signed response SRES to RAND using a one-way hash function A3 under control of the subscriber authentication key  $K_i$ . The key  $K_i$  is shared only by the subscriber and an authentication center which serves the subscriber's home network. That is, the authentication center includes all subscriber authentication keys  $K_i$ s.

Owens et al. is silent on how the keys wind up at the mobile station (mobile telephone). However, Owens et al. holds that the use of these keys is analogous to the ESN used in AMPS systems. Because the ESN is a unique identifier that is hard-coded into each mobile telephone, it is understood that the keys of Owen also are hard-coded into each mobile telephone. In addition to this assumption, Owens et al. fails to teach or suggest "a method for distributing keys" as recited in claim 1. In fact, in Owens et al. it appears that the random number challenge, and not the keys, are sent from the network to the mobile telephones.

Owens et al. is also silent on the origin of the keys. Therefore, Owens et al. neither teaches nor suggests that keys

are generated in a security device provided at the mobile radio network end.

One advantage of independent claim 1 over Owens et al. is that the subscriber can request and store a plurality of keys which he then can use as necessary. Each key may be assigned to a telecommunications service and can selectively be used to gain access to this service.

In Owens et al., each subscriber may only have a single key that is hard-coded into the subscriber's mobile telephone, rather than being distributed. While specific keys of independent claim 1 may be distributed frequently and automatically, for example, to be used for a limited purpose, for example only once.

The Examiner cites col. 16, lines 35-67 as teaching "requesting at least one key from the security device." However, this citation relates to a user entering a personal identification number (PIN) into the mobile phone, the mobile phone then forwarding the PIN, along with a number to be called, to a central server for authentication. Owens et al., and notably the section thereof cited in the Office Action, fails to teach or suggest that "at least one key is requested from the security device" as recited in claim 1.

Additionally, the Examiner states that Owens et al. teaches that the "keys are transmitted prior to providing services." The Examiner cites col. 3, lines 35-49; col. 7, lines 46-63; col. 13, lines 16-61; col. 16, lines 35-56; and figs. 8-9. In the portions of Owens et al. cited by the Examiner, number challenges are transmitted and PINs are transmitted, the dynamic PIN being generated *from* a cryptographic key, however there does not appear to be any teaching of transmitting at least one key via the mobile radio network to a mobile station or a terminal of a subscriber. Moreover, Owens et al. does not appear to teach or suggest that the transmitting of the at least one key via the mobile radio network is based on the request of a subscriber as claimed in independent claim 1 as amended.

Similarly, new independent claims 9 and 10, along with dependent claims 2-8 are patentable for at least reasons similar to the reasons stated above. More specifically, as to claims 2, 5, 6 and 9, Owen et al. neither teaches nor suggests a SIM application toolkit nor that a key transmitted via a signal channel, particularly in the form of a short message.

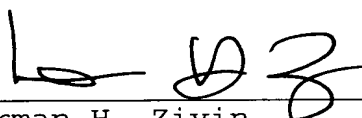
As to claims 8 and 10, Owens et al. fails to teach that a security device sends a key to one or more added value service nodes.

Therefore, by reason of the amendments made to the claims, as well as the above remarks, it is respectfully submitted that the method of distributing keys to subscribers of communications networks, as taught by the present invention and as recited in the amended claims, is neither shown nor suggested in the cited references.

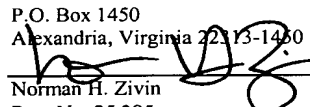
The references cited as of interest have been reviewed and are not seen to show or suggest the present invention as recited in the amended claims.

Favorable reconsideration is earnestly solicited.

Respectfully submitted,



Norman H. Zivin  
Reg. No. 25,385  
c/o Cooper & Dunham LLP  
1185 Avenue of the Americas  
New York, NY 10036  
(212) 278-0400  
Attorneys for Applicant

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to:  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
 4/1/05  
Norman H. Zivin  
Reg. No. 25,385

NHZ/JBG